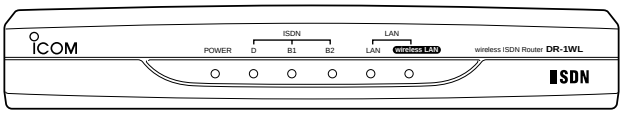
拡張機能ガイド

Firm Ver.1.7以降

Wireless ISDN Router

DR−1WL



本書は、本製品のファームウェアがバージョンアップされたことにより、追加になった機能を補足するためのガイドです。

はじめて本製品をお使いになるときには、[取扱説明書]および[活用ガイド]を先にお読みになってから、本書をお読みください。

Ver.1.6→Ver.1.7以降への主な変更点は、以下の通りです。

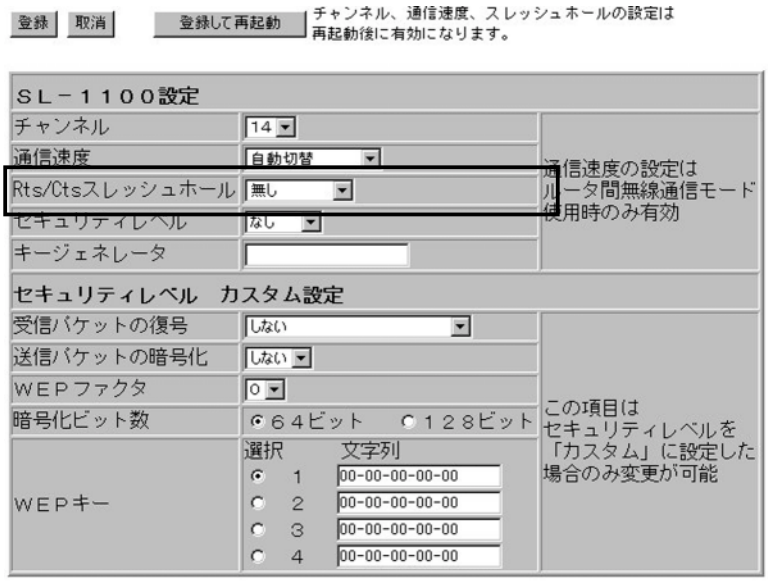
- **RADIUS(Remote Authentication Dial In User Service)に対応**
  LAN内のRADIUSサーバが使用可能
- **Rts/Ctsネゴシエーション機能**

Icom Inc.

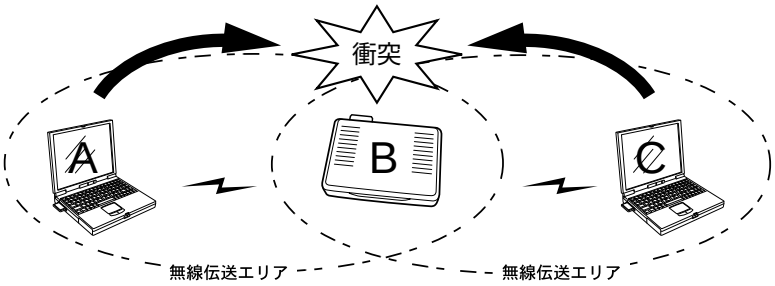
2 [SL-1100詳細設定]画面

■ 設定画面について

右記の画面は、[各種設定管理]をクリックして表示する左のフレームから、[無線LAN設定]をクリックします。さらに、右のフレーム内にある〈SL-1100詳細設定〉ボタンをクリックすると表示されます。
※[オープニング画面](☞取扱説明書)が表示されたときは、その画面の〈メニューへ〉ボタンをクリックしてから、上記の操作をします。



Rts/Ctsスレッシュホール …… ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。　(初期値：無し)
Rts/Cts(Request to send/Clear to send)スレッシュホールを設定すると、隠れ端末の影響で起こる通信速度の低下を防止できます。
隠れ端末とは、図のように、[A]と[C]の無線端末間では、互いの送信信号を受信できないので、これらを隠れ端末と呼びます。「インフラストラクチャ」モードの場合、隠れ端末が存在すると、キャリアセンス(Carrier Sense)がそれらの無線端末に有効に機能しないため、[B]の無線ルータで通信の衝突頻度が増加して、スループット(一定時間内に伝送される情報量)が低下します。
通信の衝突を防止するには、[B]の無線ルータが送信要求(Rts)信号を送信してくる相手に送信可能(Cts)信号を送ることで、無線伝送エリア内にある[A]および[C]の無線端末にCts信号が届くようになり、[B]の無線ルータが通信中は、[A]または[C]の無線端末しか[B]の無線ルータにアクセスができないようにして、通信の衝突を防止できます。



4-1.RADIUSとは

リモートアクセスで着信するユーザの認証などを本製品自身ではなくLAN側に置いたコンピューターに行わせることで、管理できる着信ユーザ数をさらにふやすために利用されます。このとき、本製品をRADIUSクライアント、認証用のコンピューターをRADIUSサーバと呼びます。

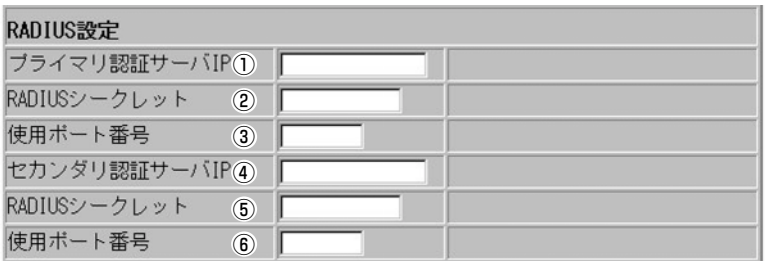
●認証について

本製品に着信するユーザの認証をRADIUSサーバによって一括管理します。また、本製品を複数で使うときなども、すべてのユーザ認証をRADIUSサーバに登録することによって一括管理できます。

本製品の[回線接続設定]画面(活用ガイド参照)で登録できる着信ユーザ数は、最大20件までですので、RADIUSサーバで管理することで、着信ユーザ登録件数をさらに増やせます。

4-2.設定画面について

右記の画面は、[ネットワーク設定]をクリックすると、右のフレームに表示されます。
※[オープニング画面](☞取扱説明書)が表示されたときは、その画面の〈メニューへ〉ボタンをクリックしてから、上記の操作をします。



①プライマリ認証サーバIP …… 最初に認証を行うRADIUSサーバのIPアドレスを入力します。
IPアドレスは、×××.×××.×××.×××の形(×：数字)で入力します。

②RADIUSシークレット …… プライマリとしてRADIUSサーバに設定している秘密鍵と同じ文字列を入力します。

③使用ポート番号 …… プライマリRADIUSサーバ側のUDPポートを指定するとき、その番号を入力します。
何も入力しないと、「1812」がUDPポートとして設定されます。

④セカンダリ認証サーバIP …… プライマリRADIUSサーバで認証できないとき、次に問い合わせを行うRADIUSサーバのIPアドレスを入力します。
入力の形は、プライマリ認証サーバアドレスのときと同じです。

⑤RADIUSシークレット …… セカンダリとしてRADIUSサーバに設定している秘密鍵と同じ文字列を入力します。

⑥使用ポート番号 …… プライマリRADIUSサーバ側のUDPポートを指定するとき、その番号を入力します。
何も入力しないと、「1812」がUDPポートとして設定されます。

4-3.設定例について

【ルータの条件】

リモートアクセス用IPアドレス

- 192.168.0.100
- 192.168.0.101

認証プロトコル

- RADIUS

【着信ユーザの条件】

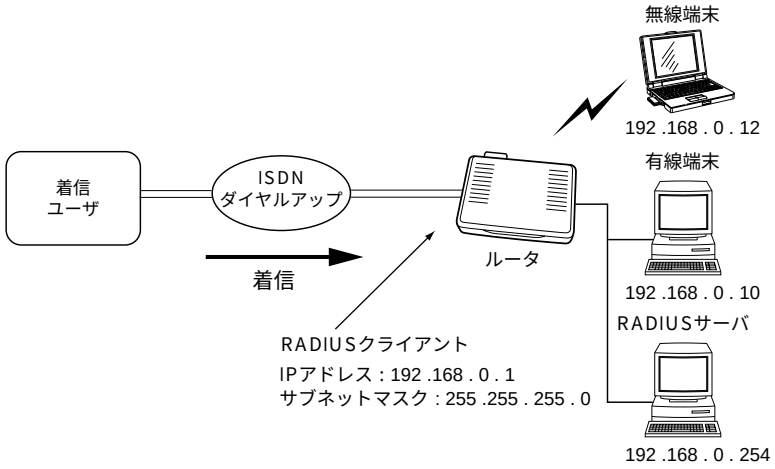
- ISDNダイヤルアップ接続
- PPPソフトのインストール
- TAまたはISDNカードの装着

【RADIUSサーバの認証条件】

ユーザ着信を許可するユーザのIDとパスワードが登録している

操作前の状態

本製品に外部からダイヤルアップを行ってきたユーザに対して、本製品がネットワーク上のRADIUSサーバ(UNIX、WindowsNT)に認証を求めます。そのユーザの着信を許可するかどうかを、そのサーバが応答する場合の設定例を説明します。
なお、クライアントとサーバ間は、TCP/IPで接続できることが前提です。



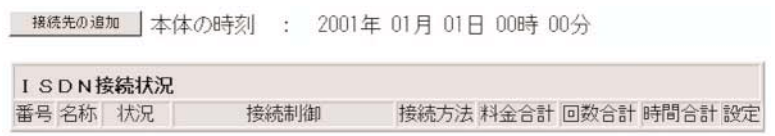
接続先として、リモートアクセスして着信してくるユーザの設定を追加します。

【手順】

1.[ISDN接続状況]画面の表示

[操作]

WWWブラウザを起動して、http://192.168.0.1をURLに指定します。



2.新規接続先画面の表示

※リモートアクセス用として、接続先を追加します。

①〈接続先の追加〉をクリック

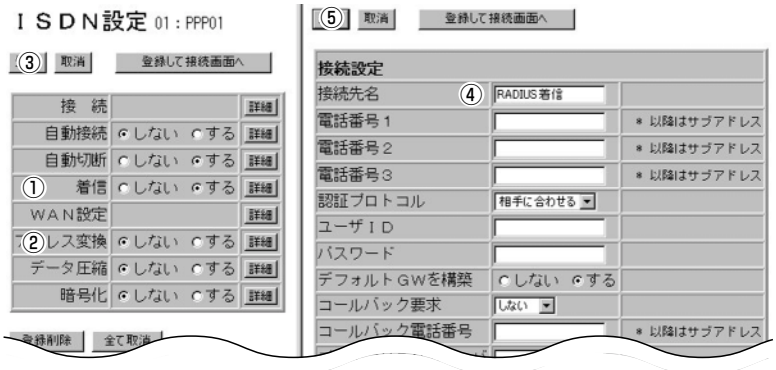
3.着信、アドレス変換、着信ユーザ名称の設定

[操作]

①着信〈する〉をクリック
②アドレス変換〈しない〉をクリック
③〈登録〉をクリック

[設定例]

④RADIUS着信(任意でよい)
⑤〈登録〉をクリック



4.着信詳細設定

[操作]

①〈詳細〉をクリック

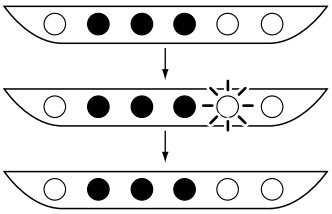
②電話番号チェック〈しない〉をクリック

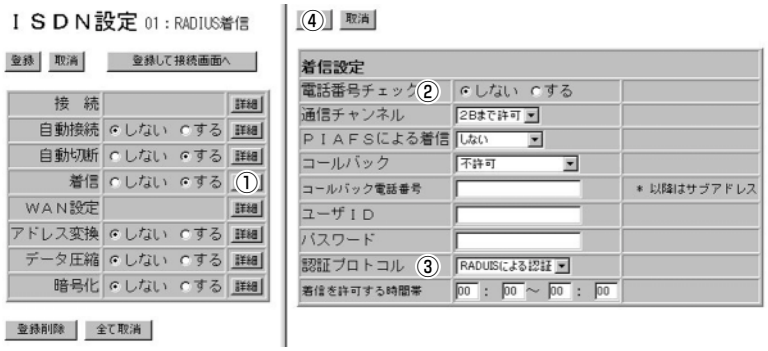
[確認]

③認証プロトコル
RADIUSによる認証
※RADIUSによる認証を選ぶと、この項目の上にあるユーザIDとパスワードを設定しても無効です。

[操作]

④〈登録〉をクリック





登録後、次の画面で、設定内容を確認します。

5.リモートアクセス用IPアドレスの設定

[操作]

①[ネットワーク設定]をクリック

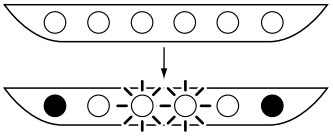
②リモートアクセスサーバを使用〈する〉をクリック

[設定例]

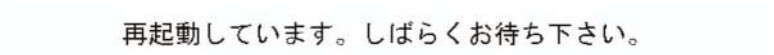
③192.168.0.100

④192.168.0.101

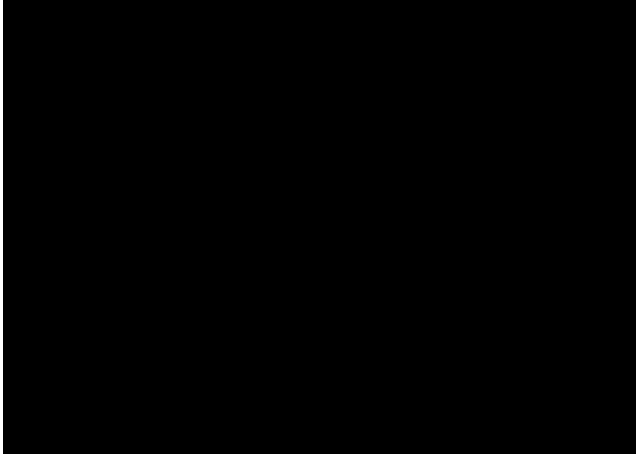
⑤〈登録して再起動〉をクリック



6.設定画面を閉じる。



高品質がテーマです。



アイコム株式会社

本　　社	547-0003	大阪市平野区加美南1-1-32	
北海道営業所	060-0041	札幌市中央区大通東9-14	TEL 011-251-3888
仙台営業所	983-0857	仙台市宮城野区東十番丁54-1	TEL 022-298-6211
東京営業所	130-0021	東京都墨田区緑1-22-14	TEL 03-5600-0331
名古屋営業所	466-0015	名古屋市昭和区御器所通2-24	TEL 052-842-2288
大阪営業所	547-0004	大阪市平野区加美鞍作1-6-19	TEL 06-6793-0331
広島営業所	733-0842	広島市西区井口3-1-1	TEL 082-501-4321
四国営業所	760-0071	高松市藤塚町3-19-43	TEL 087-835-3723
九州営業所	815-0032	福岡市南区塩原4-5-48	TEL 092-541-0211

● サービスについてのお問い合わせは各営業所サービス係宛にお願いします。

A-5686 I-3J-① © 1999 Icom Inc.